REMARKS

Claims 1-4 and 6-35 are currently pending in the subject application and are presently under consideration. Claims 1, 20, 28 and 33-35 have been amended as shown on pp. 2-8 of the Reply. Claims 3 and 19 have been canceled.

Applicants' representative thanks the Examiner for the courtesies extended during the teleconference of April 1, 2008.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-4 and 6-19 Under 35 U.S.C. §101

Claims 1-4 and 6-19 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Applicants' representative respectively disagrees.

Further, independent claim 1 has been amended herein to clearly illustrate that elements within such claims are components associated with a computer processor. In particular, claim 1 as amended is directed towards a system comprising ***a computer processor for executing the following components:*** a component that receives a first code designed in a noise model, a transformation component, a decoder and a tracing component, wherein the components perform a function (*e.g.,* receive a first code, transform the first code into a new code, determine the first code from the new code and determine whether a user accessing the first code is a valid code). (Support for these amendments can be found on pg. 7, lines 1-14 and pg. 24, lines 21-28). Accordingly, this claim includes functional descriptive material within a computer processor, thereby rendering it structurally and functionally interrelated to the computer processor and is therefore directed to statutory subject matter. Accordingly, this rejection should be withdrawn.

II. Rejection of Claims 1-4, 11, 12, 20, 26-28, 31 and 33-35 Under 35 U.S.C. §103(a)

Claims 1-4, 11, 12, 20, 26-28, 31 and 33-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Manferdelli *et al* (US 7,051,200) in view of Holthaus *et al* (US 6,229,897). It is respectfully requested that this rejection should be withdrawn for at least the following reasons. Manferdelli *et al.* and Holthaus *et al.*, individually or in combination, do not teach or suggest each and every element as set forth in the subject claims.

The claimed subject matter relates to a first code that is designed within the noise model, and performs various algebraic transformations on such first code to create a second code. Upon transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Thus the first code can be associated with error correction/detection properties when random noise is applied to the first code.

Independent claim 1 recites a system that facilitates efficient code construction, comprising: *a component that receives a first code designed in a noise model,...; and a transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, ...,* ***wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code, this allows the first code to act as it was designed to and utilize the algorithms to correct the noise errors with a high success rate****;...; and* ***a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied****.* Manferdelli *et al.* and Holthaus *et al.*, individually or in combination, do not expressly or inherently disclose the aforementioned novel aspects of applicants' claimed subject matter as recited in the subject claims.

Manferdelli *et al.* discloses a system and method for creating and using a software-based secure repository, such as a black box. The black box provided uses cryptographic techniques, such as public/private key techniques, to perform decryption and authentication services in a secure manner that resists discovery of secret keys used by the cryptographic techniques. (*See* col. 1, lines 45-52).

In contrast, applicants' claimed subject matter discloses a system that includes a tracing component. Upon decoding code 2 to retrieve code 1, the tracing component determines whether

a user accessing the code is a valid user. For example, intellectual property in a digital format (*e.g.,* mp3 files, picture files, video files, …) often includes watermarks or other suitable security mechanism that can be reviewed by a digital media player or image viewer. Accordingly, each digital media file can have a unique watermark embedded therein, wherein the watermark is associated with a particular user. A database can be generated that indexes disparate media file types, and such database can be accessed upon a media player receiving a request to play/copy/transfer a particular digital media file. If the watermark does not correlate to an authorized user of the file, then the media player can refuse to play/copy/transfer the file.

Conventional systems are not capable of robust tracing, as sophisticated users would direct attacks at a watermark until the media player would no longer recognize such watermark. As an adversary would be attacking a randomization of the digital media file, however, such adversary would be unable to determine a location of the watermark in applicants' claimed subject matter. Furthermore, if the adversary attempted an attack on the randomized code, he would be risking ruining at least a portion of the file that he is desirably playing/copying/transferring. (*See* pg. 11, lines 12-31).

Manferdelli *et al.* does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user. Accordingly, a unique watermark associated with a particular user is embedded therein. Manferdelli *et al.* simply provides error correcting code, wherein minor modifications to the code can be detected and corrected. These errors can be brought about innocently by random noise or nefariously by deliberate attacks on the code.

Accordingly, Manferdelli *et al.* is silent with regard to a system that facilitates efficient code construction, comprising: …, ***a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied***.

Holthaus *et al.* does not cure the deficiencies of Manferdelli *et al.* Holthaus *et al.* discloses an apparatus and method for providing security for analog audio communications, including voice communications over radio or landline and/or cellular telephony systems. The method includes scrambling the audio and generating a masking signal which is linearly

combined with the scrambled audio. When transmitted, the channel would appear to be noise. (*See* col. 3, lines 1-10). Whereas, applicants' claimed subject matter discloses a plurality of codes that are designed in the noise model (*e.g.,* designed knowing that the codes would be subject to random noise attacks but not adversarial attacks) that operate with a high level of performance. Applicants' claimed system utilizes these known noise model codes and transforms such codes to enable them to be associated with a high level of performance when employed in the presence of an adversary that is attacking the code.

More particularly, the claimed subject matter utilizes a first code that is designed within the noise model, and performs various algebraic transformations on such first code to create a second code. For example, one or more pseudo-random functions can be employed to transform the first code into the second code. Upon transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Thus the first code can be associated with error correction/detection properties when random noise is applied to the first code. (*See* pg. 3, line 27-pg. 4, line 16).

Holthaus *et al.* merely discloses scrambling the audio and generating a masking signal which is linearly combined with the scrambled audio. The combined scrambled audio and masking signal is then filtered and converted to analog. This scrambled/masked audio analog signal is then transmitted over the communications network. Anyone intentionally or unintentionally locking onto the channel would hear the equivalent of white nose. If the masking signal were removed, the scrambling would provide a security against someone obtaining the content of the speech. (*See* col. 5, lines 16-52).

In contrast, applicants' claimed subject matter protects against adversarial attacks and noise attacks, by treating the adversarial attacks as noise attacks. Upon transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Because random noise attacks are not concentrated on a particular

location within a code, whereas adversarial attacks are designed to destroy the mathematical property of the code, codes designed against random attacks are associated with performance that is roughly twice better than codes designed against adversarial attacks, as error detection and correction codes are well equipped to detect and recover data altered due to random noise. (*See* pg. 3, lines 3-14). Holthaus *et al.* merely scrambles audio signals to create the equivalent of white noise.

Accordingly, Holthaus *et al.* is silent with respect to a system that facilitates efficient code construction …, ***wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code, this allows the first code to act as it was designed to and utilize the algorithms to correct the noise errors with a high success rate***;...

Furthermore, independent claim 20 recites a system that hides a codeword from a computationally bounded adversary, comprising: *a code generator that generates a first code designed in a noise model and based at least in part upon a sequence of messages that are desirably relayed to a receiver,...* , ***wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code, this allows the first code to act as it was designed to and utilize the algorithms to correct the noise errors with a high success rate; and a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied***.

As stated *supra*, Manferdelli *et al.* does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user. Manferdelli *et al.* simply provides error correcting code, wherein minor modifications to the code can be detected and corrected. These errors can be brought about innocently by random noise or nefariously by deliberate attacks on the code. And, Holthaus *et al.* merely discloses scrambling the audio and generating a masking signal which is linearly combined with the scrambled audio. The

combined scrambled audio and masking signal is then filtered and converted to analog. This scrambled/masked audio analog signal is then transmitted over the communications network. Anyone intentionally or unintentionally locking onto the channel would hear the equivalent of white nose. In contrast, applicants' claimed subject matter protects against adversarial attacks and noise attacks, by treating the adversarial attacks as noise attacks.

Further, independent claim 28 recites a method for hiding a data package from a computationally bounded adversary, comprising:*...; algebraically transforming the encoded message into a first code, the first code rendered random to an unauthorized user, and the first code comprising algorithms utilized to correct noise errors with high probability; transforming the first code to a second code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary,* ***wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code; utilizing the algorithms of the first code to correct the noise errors with a high success rate; and determining whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied****.*

Manferdelli *et al.* does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user. Manferdelli *et al.* simply provides error correcting code, wherein minor modifications to the code can be detected and corrected. And, Holthaus *et al.* merely discloses scrambling the audio and generating a masking signal which is linearly combined with the scrambled audio. The combined scrambled audio and masking signal is then filtered and converted to analog. Anyone intentionally or unintentionally locking onto the channel would hear the equivalent of white nose. In contrast, applicants' claimed subject matter protects against adversarial attacks and noise attacks, by treating the adversarial attacks as noise attacks.

Further, independent claim 33 recites a system that facilitates efficient code construction, comprising: ...***wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first***

code and not concentrated on a particular location within the first code; means for utilizing the algorithms of the first code to correct the noise errors with a high success rate; and means for determining whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code.

As stated *supra*, Manferdelli *et al.* does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user. Manferdelli *et al.* simply provides error correcting code, wherein minor modifications to the code can be detected and corrected. These errors can be brought about innocently by random noise or nefariously by deliberate attacks on the code. And, Holthaus *et al.* merely discloses scrambling the audio and generating a masking signal which is linearly combined with the scrambled audio. The combined scrambled audio and masking signal is then filtered and converted to analog. This scrambled/masked audio analog signal is then transmitted over the communications network. Anyone intentionally or unintentionally locking onto the channel would hear the equivalent of white nose. In contrast, applicants' claimed subject matter protects against adversarial attacks and noise attacks, by treating the adversarial attacks as noise attacks.

Further, independent claim 34 recites a computer readable medium having computer executable instructions stored thereon to transfer a first code into a second code, ...***wherein the first code comprises a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user.***

Manferdelli *et al.* does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user, but simply provides error correcting code, wherein minor modifications to the code can be detected and corrected. And, Holthaus *et al.* merely discloses scrambling the audio and generating a masking signal which is linearly combined with the scrambled audio. The combined scrambled audio and masking signal is then filtered and converted to analog. In contrast, applicants' claimed subject matter protects against adversarial attacks and noise attacks, by treating the adversarial attacks as noise attacks.

Furthermore, independent claim 35 recites a computer readable medium having a data structure stored thereon that receives a first code that is designed in a noise model and transforms the first code into a second code, ...***wherein a tracing component is embedded in the first code that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user.***

As stated *supra*, Manferdelli *et al.* does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user, but simply provides error correcting code. And, Holthaus *et al.* merely discloses scrambling the audio and generating a masking signal which is linearly combined with the scrambled audio. The combined scrambled audio and masking signal is then filtered and converted to analog. In contrast, applicants' claimed subject matter protects against adversarial attacks and noise attacks, by treating the adversarial attacks as noise attacks.

In view of the aforementioned deficiencies of Manferdelli *et al.* and Holthaus *et al.*, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 1, 20, 28 and 33-35 (and claims 2-4, 11, 12, 26-27 and 31 which respectively depend there from).

III. Rejection of Claims 13-19, 30 and 32 Under 35 U.S.C. §103(a)

Claims 13-19, 30 and 32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Manferdelli *et al* (US 7,051,200) in view of Holthaus *et al* (US 6,229,897) in further view of Venkatsesan *et al* (US 6,829,710). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Manferdelli *et al.*, Holthaus *et al.* and Venkatsesan *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Venkatsesan *et al.* does not make up for aforementioned deficiencies of Manferdelli *et al.* and Holthaus *et al.* with respect to independent claims 1 and 28 (which claims 13-19, 30 and 32 depend respectively there from). Specifically, Venkatsesan *et al.* merely discloses providing a water mark that is associated with a pre-defined function of the code. In contrast, applicants' claimed subject matter discloses a unique watermark embedded within the first code and *associated with a particular user*. If the watermark does not correlate to an authorized user of the file, then access is denied. Thus, the claimed subject matter as recited in claims 13-19, 30 and 32 is not obvious over the combination of Manferdelli *et al.*, Holthaus *et al.* and Venkatsesan *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

IV. Rejection of Claims 6-8 and 28-29 Under 35 U.S.C. §103(a)

Claims 6-8 and 28-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Manferdelli *et al* (US 7,051,200) in view of Holthaus *et al* (US 6,229,897) in further view of Cox

et al (US 6,275,965). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Manferdelli *et al.*, Holthaus *et al.* and Cox *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Cox *et al.* does not make up for aforementioned deficiencies of Manferdelli *et al.* and Holthaus *et al.* with respect to independent claims 1 and 28 (which claims 6-8 and 29 depend respectively there from). Thus, the claimed subject matter as recited in claims 6-8 and 28-29 is not obvious over the combination of Manferdelli *et al.*, Holthaus *et al.* and Cox *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

V. Rejection of Claims 9 and 10 Under 35 U.S.C. §103(a)

Claims 9 and 10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Manferdelli *et al* (US 7,051,200) in view of Holthaus *et al* (US 6,229,897) in further view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Manferdelli *et al.*, Holthaus *et al.,* and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned deficiencies of Manferdelli *et al.* and Holthaus *et al.* with respect to independent claim 1 (which claims 9 and 10 depend there from). Thus, the claimed subject matter as recited in claims 9 and 10 is not obvious over the combination of Manferdelli *et al.*, Holthaus *et al.* and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

VI. Rejection of Claims 21-23 Under 35 U.S.C. §103(a)

Claims 21-23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Manferdelli *et al* (US 7,051,200) in view of Holthaus *et al* (US 6,229,897) in further view of Bohnke (US 6,557,139). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Manferdelli *et al.*, Holthaus *et al.* and Bohnke *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Bohnke *et al.* does not make up for aforementioned deficiencies of Manferdelli *et al.* and Holthaus *et al.* with respect to independent claim 20 (which claims 21-23 depend there from). Thus, the claimed subject matter as recited in claims 21-23 is not obvious over the

combination of Manferdelli *et al.*, Holthaus *et al.* and Bohnke *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

VII. Rejection of Claim 24 Under 35 U.S.C. §103(a)

Claim 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Manferdelli *et al* (US 7,051,200) in view of Holthaus *et al* (US 6,229,897) and Bohnke (US 6,557,139) in further view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Manferdelli *et al.*, Holthaus *et al.*, Bohnke *et al.,* and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned deficiencies of Manferdelli *et al.*, Holthaus *et al.* and Bohnke *et al.* with respect to independent claim 20 (which claim 24 depends respectively there from). Thus, the claimed subject matter as recited in claim 24 is not obvious over the combination of Manferdelli *et al.*, Holthaus *et al.*, Bohnke *et al.* and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP588US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731